SUPREME COURT OF QUEENSLAND

CITATION:	*R v Boden* [2002] QCA 164
PARTIES:	**R** **v** **BODEN, Vitek** (applicant/appellant)
FILE NOS:	CA No 324 of 2001 DC No 340 of 2001
DIVISION:	Court of Appeal
PROCEEDING:	Appeal against Conviction and Sentence
ORIGINATING COURT:	District Court at Maroochydore
DELIVERED ON:	10 May 2002
DELIVERED AT:	Brisbane
HEARING DATE:	21 March 2002
JUDGES:	Davies JA, Muir and Wilson JJ Separate reasons for judgment of each member of the Court, each concurring as to the orders made
ORDER:	**Appeal against conviction allowed in part. Convictions on counts 21 to 26 inclusive set aside. Application for leave to appeal against sentence dismissed.**
CATCHWORDS:	CRIMINAL LAW – APPEAL AND NEW TRIAL AND INQUIRY AFTER CONVICTION – APPEAL AND NEW TRIAL – PARTICULAR GROUNDS - UNREASONABLE OR INSUPPORTABLE VERDICT – WHERE EVIDENCE CIRCUMSTANTIAL – where appeal against conviction – where appellant argued insufficient and incorrect evidence and that lies were taken into account and that evidence was tampered with – where strong Crown case established – whether conclusions reached were open to jury on evidence at trial CRIMINAL LAW – APPEAL AND NEW TRIAL AND INQUIRY AFTER CONVICTION – APPEAL AND NEW TRIAL – APPEAL AGAINST SENTENCE – APPEAL BY CONVICTED PERSONS – APPLICATIONS TO REFUSE SENTENCE – WHEN REFUSED – GENERALLY - where deliberate conduct over several weeks – where appellant aware that harm could occur – where intent to cause damage established – whether sentence manifestly excessive *Criminal Code* (Qld), s 408D

Domican v The Queen (1991-1992) 173 CLR 555, considered
RPS v The Queen (2000) 199 CLR 620, considered

COUNSEL: The applicant/appellant appeared on his own behalf
C W Heaton for the respondent

SOLICITORS: The applicant/appellant appeared on his own behalf
Director of Public Prosecutions (Queensland) for the respondent

[1] **DAVIES JA:** I agree with the reasons for judgment of Muir J and with the orders he proposes.

[2] **MUIR J:** After a trial in the District Court the appellant, who appeals against conviction and seeks leave to appeal against sentence, was convicted of –

> 26 counts of using a restricted computer without the consent of its controller thereby intending to cause detriment or damage;
>
> 1 count of using a restricted computer without the consent of its controller intending to cause detriment or damage and causing detriment greater than $5,000;
>
> 1 count of wilfully and unlawfully causing serious environmental harm; and
>
> 1 count of stealing a two-way radio and 1 count of stealing a PDS compact 500 computer.

[3] He was sentenced on 31 October 2001 to imprisonment for –

> 18 months on each of the 26 counts;
>
> 2 years imprisonment on the count involving damage greater than $5,000;
>
> 12 months imprisonment on the environmental harm count;
>
> 6 months imprisonment on each of the counts of stealing.

All sentences were ordered to be served concurrently.

For convenience, I will refer to the counts involving the use of computers as computer hacking counts or charges.

Summary of the prosecution evidence

[4] The evidence was heard over a 9 day period. The appellant withdrew his legal representatives' instructions before the commencement of the second day of the trial

and thereafter represented himself. Thirteen witnesses were called in the Crown case and the appellant elected not to give or call evidence on his behalf.

[5] The Crown case on the computer hacking offences was that between 9 February 2000 and 23 April 2000 the appellant accessed computers controlling the Maroochy Shire Council's sewerage system, altering electronic data in respect of particular sewerage pumping stations and causing malfunctions in their operations.

[6] The evidence revealed that the Council's sewerage system had about 150 stations pumping sewerage to treatment plants. Each pumping station had installed a PDS Compact 500 computer capable of receiving instructions from a central control centre, transmitting alarm signals and other data to the central computer and providing messages to stop and start the pumps at the pumping station. Communications between pumping stations and between a pumping station and the central computer were by means of a private two-way radio system operating through repeater stations at Buderim, Nambour and Mount Coolum. Each repeater station transmitted on a different frequency.

[7] Hunter Watertech Pty Ltd installed the computerised system over a period of about two and a half years. By mid January 2000 the installation work had been completed but the system still had some teething problems receiving attention.

[8] The appellant, an engineer, had been employed by Hunter Watertech as its site supervisor on the project for about two years until resigning with effect from 3 December 1999. At about the time of his resignation he approached the Council seeking employment. He was told to enquire again at a later date. He made another approach to the Council for employment in January 2000 and was told that he would not be employed. The sewerage system then experienced a spate of faults. Pumps were not running when they should have been, alarms were not reporting to the central computer and there was a loss of communication between the central computer and various pumping stations. An employee of Hunter Watertech, Mr Yager, was appointed to look into the problem. He began monitoring and recording all signals, messages and also traffic on the radio network. As a result of his investigations he concluded that many of the problems being experienced with the system resulted from human intervention rather than equipment failure. His opinion was shared by other technical experts who gave evidence. Further, the evidence revealed that the problems associated with the alleged hacking ceased when the appellant was arrested.

[9] On an occasion during Mr Yager's investigations he ascertained that pumping station 14 seemed to be the source of the messages corrupting the system. He physically checked the pumping station and ascertained that it was working properly and bore no signs of having been tampered with. He concluded that the source of the false messages was a PDS Compact 500 computer with an address of 14 and he changed the identification number of pumping station 14 to 3 so that any legitimate messages from that station could be identified as coming from station 3. Conversely, any messages coming from a station identifying itself as 14 would be known to be bogus. "PDS Compact 500" is Hunter Watertech's brand name for the computer device installed by it at each pumping station and which is connected by radio link to the central computer.

[10] On 16 March 2000, when malfunction occurred in the system, Mr Yager communicated over the network with a bogus pump station 14 which was sending messages to corrupt the system. He was temporarily successful in altering his programme to exclude the bogus messages but then had his computer shut out of the network for a short period. The intruder was now using PDS identification number 1 to send messages.

[11] Further problems then occurred as a result of a person gaining computer access to the system and altering data so that whatever function should have occurred at affected pumping stations did not occur or occurred in a different way. The central computer was unable to exercise proper control and, at great inconvenience and expense, technicians had to be mobilised throughout the system to correct faults at affected pumping stations. On the occasion the subject of count 45, a pumping station overflowed causing raw sewerage to escape.

[12] On 23 April 2000 an intruder, by means of electronic messages, disabled alarms at four pumping stations using the identification of pumping station 4. The intrusions began just after 7:30 pm and concluded just after 9:00 pm.

[13] By this time the appellant had fallen under suspicion and was under surveillance. A vehicle driven by him was located by police officers on the Bruce Highway near the Glasshouse Mountains heading south. A police car started to follow the appellant's vehicle which then turned off the highway at the Deception Bay exit. The police car missed the turn, turned around and started to go the wrong way up the exit ramp in order to follow the appellant when his vehicle was seen coming down the ramp to the highway. When the appellant's vehicle was pulled over and searched at around 10:00pm, a PDS Compact 500 computer, later identified in evidence as the property of Hunter Watertech, was found in it as was a laptop computer.

[14] On examination it was found that the software to enable the laptop to communicate with the PDS system through the PDS computer had been re-installed in the laptop on 29 February 2000 and that the PDS Compact computer had been programmed to identify itself as pump station 4 – the identification used by the intruder in accessing the Council sewerage system earlier that night. The software programme installed in the laptop was one developed by Hunter Watertech for its use in changing configurations in the PDS computers. There was evidence that this programme was required to enable a computer to access the Council's sewerage system[1] and that it had no other practical use[2].

[15] The unchallenged evidence of Mr Kingsley, a police computer expert, was that the programme had been used at least 31 times between 7 April and 19 April and that it was last used at 9:31pm on 23 April 2000. Also found in the car was a two-way radio set to the frequencies of the Buderim and Mount Coolum repeater stations and the leads necessary to connect the PDS computer, the laptop and the radio.

[16] Evidence was given by Mr Yager and others that the conduct of the person responsible for the unauthorised interventions in the computer system displayed a detailed familiarity with the system, beyond that which was likely to be held even by Council technical staff. Technical experts other than Mr Yager also gave

---

1 The evidence of Mr Lewer an engineer and project manager employed by Hunter Watertech.

2 The evidence of Mr Yager.

evidence that the computer malfunctions, the subject of the hacking charges, were the result of human intervention.

[17] When apprehended by police the appellant asserted in a taped conversation that all the items in the vehicle were his own. He said he had been up to Rainbow Beach and that the computer was used by him for study, personal correspondence and work in his family business. He later sent a letter to the police at Maroochydore requesting the immediate return of his property.

[18] Examination of the laptop found in the car revealed start up and shut down times (on and after 28 February 2000) consistent with use at the time of the attacks which Mr Yager had uncovered and which he had logged.

Conclusions as to the strength of the Crown case

[19] The evidence which I have discussed did not directly establish that the appellant had sent the messages which corrupted the operation of the Council's sewerage system and which are the subject of the counts on which the appellant was found guilty. In the absence of evidence from the appellant however, it did lay the foundations of a strong circumstantial case. Evidence or explanation of damning inferences the jury was entitled to draw from the facts proved by the Crown could come only from the accused and in the absence of such evidence or explanation the jury could more readily return a guilty verdict[3]. The learned trial judge in his sentencing remarks described the Crown case as "an extremely strong one, almost overwhelming".

The grounds of appeal

[20] Against this background I turn to a consideration of the matters raised by the appellant in support of his appeal against conviction.

1. There was insufficient evidence to show that problems attributed by the prosecution to hacking were done by the accused or anyone else. Witnesses were lying or making up stories to help the prosecution.

[21] As I have said, the prosecution mounted a strong circumstantial case. Mr Yager's evidence was that the matters the subject of the counts on which the appellant was found guilty arose through human intervention. His opinions do not appear to have been shaken in cross-examination and were supported by the evidence of other witnesses. Not only was that evidence uncontradicted by other evidence, there was cogent evidence linking the appellant with the hacking.

2. The equipment installed by Hunter Watertech had continuous problems before and after the appellant's arrest so that the malfunctions relied on by the prosecution can't be attributed to improper intervention beyond reasonable doubt.

[22] In support of this ground the appellant points to various passages in the evidence which he contends support the conclusion that the subject equipment suffered problems from time to time.

---

3 c.f. *RPS v The Queen* (2000) 199 CLR 620 at 633.

[23] The existence of other problems in the system may have made it more difficult for the prosecution to prove its case, but there is evidence, which it was open to the jury to accept, which showed that the malfunctions relied on by the prosecution were the result of human intervention. Once it was demonstrated that the subject malfunctions resulted from human intervention the existence of other problems became of limited significance. Again, the jury was entitled to assess the evidence of Mr Yager and the other expert witnesses in light of the fact that no contradictory evidence was led by the appellant.

[24] Mr Yager was adamant that the malfunctions in the system which were the subject of the charges could only have been caused by unauthorised human intervention. He maintained this position throughout his cross-examination. Mr Lewer's evidence was to like effect. He is an engineer specialising in computer engineering who, for a time, was Hunter Watertech's project engineer on the installation of the computerised sewerage system.

[25] During the trial and on appeal the appellant sought to establish that some of the electronic messages which gave rise to the charges could have been caused by system malfunction or by error on the part of Council employees. One of his arguments in this regard was made by reference to exhibits 26, 27 and 28. The latter (which reproduced in print much less than one thousandth of the record from which it was extracted) showed three sets of identical messages on the same day from addresses 000, 099 and 004.

[26] The Crown contended that only the message emanating from address 004 was initiated by the accused. The accused, pointed to the other messages as evidence that defective messages of the nature of those relied on by the Crown may have been caused other than by human intervention.

[27] Mr Lewer said, and the appellant appeared to accept, that all three messages were generated by the PDS config programme used on the PDS Compact computers. Mr Lewers opinion was that the messages, other than the ones from address 004, were generated by persons attempting to rectify the result of the alleged unauthorised intervention. He also gave evidence that that 000 and 099 messages were not causing damage to the computer system.

[28] Mr Yager gave evidence some days later than Mr Lewer and thus had more opportunity to consider the possible explanations for the 000 and 099 messages. His evidence was that these messages occurred over several days and resulted from the actions of maintenance staff who were either employees of Hunter Watertech or Council employees under direction of the former. He ruled out the possibility of mechanical error. He said that the 004 messages were definitely generated by a person different from the one who generated the other messages. He does not appear to have been challenged in cross examination by the appellant on that point.

3. The corruptions in the Coolum area on 26 March 2000 were caused by technical problems.

[29] The contentions of the appellant in this regard repeat, to a substantial degree, matters addressed under the previous heading. As has already been stated, it is insufficient for the appellant to point to the possibility or even probability of errors within the system which were not caused by human intervention. The prosecution's

case accepted the existence of various malfunctions but relied on the evidence of Mr Yager and Mr Lewer, in particular, to attribute specific malfunctions to the intervention of the appellant. That was the case in relation to the relevant events of 26 March and the other matters the subject of the other hacking counts. There was evidence, which it was open to the jury to accept, which identified the matters the subject of counts 44 and 45 as the result of hacking.

4. The appellant was convicted on counts 21 to 46, which concerned events which were alleged to have commenced on 28 February 2000. On that day the appellant reloaded the windows software on his computer and the computer could not have been used for hacking on that day.

[30] The counts on which the appellant was found guilty related to acts of hacking which commenced on or about 28 February.

[31] Mr Kingsley's evidence was that he examined the laptop taken by the police from the appellant's vehicle and also the software loaded on it. He found that the laptop had been reloaded with most of its software operating programmes on 28 February 2000. He was unable to identify what had been on the laptop prior to 28 February but concluded that the laptop had been in use before 28 February, that it had been affected by "the Chernobyl virus", that this had probably happened on 26 February and that the effects of the virus had caused the operator of the computer to reload it.

[32] Mr Kingsley found also that a PDS software file had been installed or re-installed on the laptop on 29 February at 15:46 hours. His evidence was that this is the software used to run or access the computers in the sewerage system. An electronic log located by Mr Kingsley revealed that the programme had been run at least 31 times prior to 19 April, the date on which the log was made. He was also able to show that the programme had been last run on 23 April at 9:31pm.

[33] The appellant made no complaint in his grounds of appeal by reference to the software loaded on 29 February. His complaint is that the computer couldn't be used on the 28th because the software was reloaded that day.

The appellant was acquitted on all counts relating to hacking prior to 28 February but convicted on all counts relating to hacking after that date. Counts 21 to 26 inclusive concerned hacking alleged to have occurred "on or about 28 February 2000". The acts relied on by the Crown in fact occurred on 28 February.

[34] The learned crown prosecutor submitted that the conduct of the jury in convicting the appellant for offences committed on or after 28 February 2000 could be explained by the evidence of re-installation of software on 28 February. That appraisal however, overlooks the evidence that the PDS software was not installed until the following day.

[35] In his careful and detailed summing up the learned trial judge reminded the jury of the installation of files in the computer on 28 February but omitted to mention the evidence of installation or re-installation of the PDS software on 29 February. That was probably because little emphasis was given to the loading of the PDS software in the course of the evidence. There was no cross-examination on the point.

[36] The trial judge was not obliged to canvass all the evidence in his summing up. As was observed in the joint judgment in *Domican v The Queen*[4].

> "Whether the trial judge is bound to refer to an evidentiary matter or argument ultimately depends upon whether a reference to that matter or argument is necessary to ensure that the jurors have sufficient knowledge and understanding of the evidence to discharge their duty to determine the case according to the evidence. Consequently, the conduct of the case necessarily bears on the extent to which the judge is bound to comment on or discuss the evidence. Discussion or comment which is justified or required in one case may be neither required nor justified when a similar case is conducted in a different way".

[37] The jury was reminded, quite properly, of the evidence of the installation of programme files in the accused's laptop on 28 February and of the possibility that the re-loading occurred as a result of the computer being affected by a virus on 26 February. That evidence was of significance in relation to the question of whether the appellant could have used the computer for hacking on 28 February. But the re-loading of the PDS programme on the following day was also directly relevant to that question. Reminding the jury of one part of these interrelated pieces of evidence and not the other gave rise to a risk that the jury might overlook the evidence in relation to the PDS programme or not appreciate its significance.

[38] Moreover, as each of the counts on the indictment concerned hacking alleged to have taken place on or about a specified day or specified days it was desirable in the summing up to direct the jury's attention to evidence which bore upon the question of whether hacking by the appellant could be established on those days. Unless that was done it was possible that the jury might overlook the fact that a necessary element of each offence was that alleged events took place on or about a particular date and tend to make an assessment based on whether hacking generally had been proved against the appellant.

[39] The trial presented the jury with issues of some complexity. The bulk of the evidence was technical in nature and much of it involved concepts beyond the knowledge even of persons with a basic working knowledge of computer operations. As was noted earlier, 13 witnesses gave evidence over nine days and for all but one of those days the appellant appeared for himself. He did not address at the conclusion of the trial and nor did the Crown prosecutor. In those circumstances a heavier than usual burden to sum up the evidence for and against the Crown case fell on the trial judge.

[40] For the above reasons, I conclude that the convictions on counts 21 to 26 inclusive should be set aside as unsafe and unsatisfactory. In reaching this conclusion I am conscious of the difficulty of assessing the adequacy of a summing up remote from the atmosphere of the trial and without the trial judge's advantage of seeing and hearing the witnesses.

---

4 (1991 – 1992) 173 CLR 555 at 561

[41] The remaining counts concern matters after the 28th and 29th of February. As well, the events with which they are concerned took place whilst Mr Yager was conducting his investigations and keeping records of malfunctions. The evidence against the accused in relation to those counts is thus particularly strong and the verdicts on them are not called into question by the matters just discussed.

5. Mr Kingsley gave evidence which was incorrect in a number of respects which assisted the prosecution case.

[42] The evidence of Mr Kingsley, the police computer expert who examined the appellant's laptop, when coupled with the circumstances of the appellant's apprehension by police with the laptop PDS computer and radio in his possession, made a very convincing case against the appellant.

[43] The jury was entitled to accept the evidence of Mr Kingsley. His expertise was not successfully challenged and nor were critical aspects of his evidence. His evidence, of course, was uncontradicted.

6. The computer and other items taken from the appellant were not stored properly after being taken and were inspected by persons " with (a) vested interest". By inference it is being alleged that the evidence was tampered with.

[44] The evidence does not establish that any critical equipment or materials were corrupted in any material way. Nor did it give rise to any inference that such corruption may have taken place.

7. It was not proved that the appellant was in or about Maroochydore on the days when hacking was alleged to have occurred or that any of the illicit messages were sent by the appellant's computer.

[45] The evidence did not prove directly that the appellant was in or about Maroochydore at critical times. That fact needed to be established by inference and it was open to the jury to draw the necessary inference having regard to the evidence discussed thus far.

8. The charges of stealing were not proved in relation to the radio. It was shown that the serial number on the radio was on a list of items bought from a wholesaler by Hunter Watertech. If it had been stolen from the Council that would have been obvious immediately as one of the pumping stations would have ceased to work. It was demonstrated that the computer may have belonged to the Redlands Shire and not to Hunter Watertech.

[46] The evidence of witnesses Lewer, Stringfellow and O'Kane identified the subject equipment and it was open to the jury to accept their evidence. Mr O'Kane, State Manager of Hunter Watertech at the time of the appellant's resignation, at the request of police, went with another Hunter Watertech employee, Mr Wilkins, to the Redcliffe police station on 24 April 2000. He was there shown some equipment which included a two-way radio which he recognised as one of the type used in the Council's communication system. He observed Mr Wilkins conduct a test which demonstrated that the radio was tuned into the frequencies of the Buderim and Coolum repeaters. The serial numbers on the radio also matched one of the

numbers on a delivery docket provided by the supplier of the radios to Hunter Watertech.

[47] At the same time he was shown a PDS Compact 500 in which, when the top was removed, he was able to see was set to 004. He noticed that the device had a serial number CL149. He identified it by reference to Hunter Watertech's records as a device which should have been in the possession of Hunter Watertech. He also identified cables and a transformer retrieved by the police from the appellant and shown to him as sufficient to provide power to the radio and the computer from a motor vehicle's cigarette lighter. It will be recalled also that when apprehended by police and subsequently, the appellant asserted that the radio and PDS computer were his property.

9. The appellant had no motive for the alleged conduct.

[48] The prosecution did not have to establish a motive but there was evidence from which the jury could have concluded that a motive existed. For example, the appellant was looking for employment with the Council. He was an expert in the computer system and may have thought that if the system continued to cause difficulty the Council may have wanted to avail itself of his expertise. In his sentencing remarks the trial judge expressed the view that the appellant was actuated by a desire for vengeance.

Conclusion

[49] For all of the foregoing reasons I would allow the appeal in part and order that the convictions on counts 21 to 26 inclusive be set aside.

Sentence

[50] The appellant seeks leave to appeal against the sentence on the grounds that it was manifestly excessive. He supports his application by pointing out that he has spent two years of his life defending the accusations and that, in consequence of his conviction, his job prospects are slim.

[51] The appellant, at the time of the offences, was a professional man aged about 48 years of age. At the time of sentencing he was almost 50 years of age. He had no previous criminal history. The learned sentencing judge found that whilst it was not the appellant's "sole purpose to cause sewerage overflows and environmental harm" he was aware that such overflows could occur.

[52] The maximum penalty for each of the 26 hacking counts is five years' imprisonment[5]. For the hacking count of causing detriment greater than five thousand dollars, the maximum penalty is ten years imprisonment[6].

[53] The appellant's conduct was engaged in over a period of some weeks. It was deliberate and the appellant, when engaging in it, misused confidential information and made use of stolen property. He must have been aware that his acts would cause the Council and his former employer considerable disruption, inconvenience and expense. The cost to the Council alone was many thousands of dollars. Indeed,

---

5 s. 408D(2) of the Criminal Code

6 s. 408D(3) of the Criminal Code

it may be inferred that the conduct was calculated to cause disruption. As the trial judge pointed out, the appellant, being aware of the risk of sewerage spills, was prepared to take that risk to gain his own ends.

[54] It is implicit in the jury's verdicts that an intent to cause damage was established in each case. The sewerage spill was significant. It polluted over 500 metres of open drain in a residential area and flowed into a tidal canal. Cleaning up the spill and its effects took days and required the deployment of considerable resources. The appellant was ordered to pay $13 110.77 to the Council by way of compensation for the loss and damage cause to it by the spill. That is a relevant consideration.

[55] Having regard to the matters I have mentioned, the sentences imposed in respect of the convictions which remain, in my view, can hardly be said to be excessive, let alone manifestly excessive, particularly as public deterrence may be thought to be a significant consideration. I would dismiss the application for leave to appeal against sentence.

[56] **WILSON J:** I agree with Muir J that the appeal against conviction should be allowed in part, and I agree with the order he proposes. I would dismiss the application for leave to appeal against sentence for the reasons given by His Honour.